COMMUNITY HEALTH PLAN
of Washington™

November 2021

Compliance Program

Compliance Today

Corporate Compliance & Ethics Week

NOVEMBER 7-13, 2021
CORPORATE COMPLIANCE & ETHICS WEEK
Awareness, Recognition, Reinforcement

Corporate Compliance & Ethics Week is an annual event sponsored by the Health Care Compliance Association (HCCA) and the Society of Corporate Compliance and Ethics (SCCE) to increase awareness of compliance and ethics issues. The first 'official' Corporate Compliance & Ethics Week was observed in 2005; however, its roots can be traced back as early as 2002.

This year marks the 17th annual Corporate Compliance & Ethics Week celebration.

Community Health Plan of Washington (CHPW) has celebrated Corporate Compliance & Ethics Week since 2012. The Compliance department leads activities and educational opportunities throughout the week to interact, educate, and engage with workforce members.

The theme for 2021 is, "**Awareness, Recognition, Reinforcement.**"

Join the Compliance department in celebrating:

- Educational E-Games:
  - Compliance Crossword Puzzle
  - Identifying Compliance
  - Compliance Word Search
  - Compliance Word Scramble
  - inside CHPW Compliance Scavenger Hunt
- Daily quizzes through inside CHPW.
- Win Prizes!
  - The more you play and interact, the more chances for you to win.
  - This year's prizes will include e-gift cards from the following retailers:
    - Target
    - Starbucks
    - Amazon

For More Information:

- Corporate Compliance and Ethics Week
- HCCA, SCCE
- Compliance Department on inside CHPW

A Message from Leanne

Community Health Plan of Washington (CHPW) is committed to conducting business with the highest degree of ethics, integrity, and compliance with laws. Our ***Standards of Conduct*** set forth these commitments and provides standards for our conduct across our workforce, governing body, and our contracted partners.

Compliance Today

CHPW's Standards of Conduct are an extension of our Mission and organizational values. ***CHPW's Standards of Conduct*** go beyond complying with laws; the standards reflect our expectation that CHPW's staff, governing body, and contracted partners conduct all business with honesty, dignity, and respect for our members and that all activities are conducted with the utmost degree of integrity. ***CHPW's Standards of Conduct*** are designed to help guide us in our decision-making and activities on behalf of CHPW to ensure that we continue to meet our high ethical standards. It is important that each of us understand and follow the ***CHPW's Standards of Conduct***, comply with all applicable laws, and refrain from business situations that would place us at risk or jeopardize CHPW's integrity and reputation in the community.

Every CHPW workforce member is encouraged to report any known or suspected illegal or unethical behavior, or violations of the Standards of Conduct. CHPW provides access to a confidential, anonymous **Compliance Hotline** for workforce members to report instances of suspected or detected non-compliance, potential fraud, waste, or abuse (FWA), and other compliance and ethics concerns. The Hotline is operated and available 24 hours a day, seven days a week at **(800) 826-6762**, by NAVEX (vendor)**.** You can also make an anonymous report online by visiting the Compliance Hotline reporting site at: http://chpw.ethicspoint.com. You can access the online reporting site with the link above, visiting the 'Compliance Hotline' button from the Employee Quick Links on the *inside*CHPW home page, and from a link on the Compliance department page on *inside*CHPW.

CHPW prohibits retaliation for compliance-related questions or reports of potential non-compliance or potential FWA made in good faith. Making deliberately false or malicious reports is prohibited. If you feel you have been threatened or intimidated after making a report, or prior to making a report, notify the HR department or the VP, Compliance Officer.

Maintaining ethical conduct and complying with laws are foundational to CHPW's mission and success. We count on every workforce member to do their part by understanding and complying with the Standards of Conduct and to report any potential concerns.

CHPW's Standards of Conduct are available at: https://inside.chpw.org/departments/compliance/standardsofconduct~3

Managing Access and MAC Forms

Strong security controls and individual diligence are critical to preventing unauthorized access or disclosure of protected health information (PHI). CHPW uses role-based job descriptions and defined PHI Access Level Categories to limit workforce member access to the appropriate level of PHI, required to perform a specific function.

To ensure the appropriate level of access is granted to a workforce member, the hiring manager (or the business owner in the event of a vendor or auditor) is responsible for partnering with their HR Business Partner to complete and submit a New Hire Move, Add, and Change (MAC) Form located under the “Employee Tools” section on inside CHPW **at least five (5) business days prior to the workforce member or contractor start date**.

When there is a change in job function, it is important that the workforce member’s access be confirmed or modified based on their job description. The Change MAC Form should be submitted **at least five (5) business days prior to the workforce member’s change in job function**.

When a workforce member separates employment (voluntarily or involuntarily), the manager must submit a Departure MAC Form as soon as a separation date has been finalized, but **no later than five (5) business days prior to the workforce member’s last day of work** (in the case of voluntary separation), **or immediately** (in the case of involuntary separation) noting same-day separation.

Failure to comply with CHPW’s MAC Form process or any other security policy may result in disciplinary action as described in Corrective Action and Discipline Policy (EE204). Disciplinary action may include termination. Legal actions may also be taken if a violation of the law has occurred.

A quick training is available in UKG Pro Learning for people managers to learn about the MAC Form process. This training is not assigned; search for “MAC Form Training” in the catalogue.

For More Information:

- Employee Network and Facility Access Authorization (MAC Form Procedure) Procedure (CO335)
- Corrective Action and Discipline Policy (EE204)

Data Classification and Protection

Appropriate controls must be in place to protect data from intentional or accidental disclosure, modification, or destruction. Systems that process, store, or forward CHPW information must comply with appropriate levels of security defined for that information.

This applies to all CHPW information including, but not limited to, information that is either stored or shared by any means. This includes electronic information, information on paper, and information shared visually (such as video conferencing).

All CHPW workforce members should familiarize themselves with the information labeling and handling guidelines.

Information Classification

All CHPW information will be classified at one of three levels: **public, highly sensitive, or internal use only**.

- **Public:** this is the least restrictive classification. It is information that if disclosed, would not adversely impact CHPW, its members or staff. Examples of this information include:
    - Press releases

  - Marketing Materials
  - Public web site information
- **Highly Sensitive**: this information requires a greater level of protection to prevent loss of inappropriate disclosure. Sensitive information includes information designated by HIPAA "protected health information," and payment card information as designated by the Payment Card Industry Data Security Standard (PCI DSS). Examples include:
  - Individually Identifiable Health Information
  - Credit Card or other financial account numbers
  - Social Security Numbers
  - Driver's License Numbers
- **Internal Use Only**: this information is for organizational use only and distributed only on a "need to know" basis. This includes information where disclosure may damage the public trust placed in CHPW but would not violate any regulations. This includes information that is available to business units and used for official purposes, but in general should not be released to the public. Examples include:
  - Financial accounting information
  - Payroll information
  - Budgets
  - Contracts

Information Classification

- Each information system is to be classified according to the categories above and considering the risk associated with the data being stored or processed. All electronically stored information must have a designated data custodian. It is the data custodian's responsibility to classify the information and understand its value, legal requirements, sensitivity, and criticality to CHPW. The data custodian is normally someone who is responsible for, or dependent on, the business process associated with the information asset, and who is knowledgeable about how the information is acquired, transmitted, stored, deleted, and otherwise processed.
- Information assets must be evaluated, valued, and categorized by the data custodian on a regular basis.
- The data custodian must periodically review access rights to the information to ensure the rights are removed from any personnel no longer requiring business access. The access review frequency can be set based on the information classification (e.g., 3-month intervals, 6-month intervals, 12-month intervals).
- If information at several different classification levels exists on a computer storage media, then the system controls must reflect the requirements associated with the most restrictive data classification level.
- All information assets must be used, accessed, stored, transmitted, transported, deleted, and destroyed in a manner consistent with the requirements for the information classification level.

- The data custodian is responsible for controlling access to their information and must be consulted when other entities wish to extend access authority.

Information Protection

- Protective measures must consider the value associated with unauthorized access or loss of information assets.
- Highly Sensitive data sent across any network connection must be encrypted in accordance with the CHPW Encryption Standard.
- Private or confidential data stored in a database or file system must be encrypted in accordance with CHPW's Encryption Standard Procedure (IT133) unless an exception is granted by the Security Officer. Any exceptions must be reviewed annually.

For More Information:

- Data Classification and Protection Policy (IT136)

Conflicts of Interest

A conflict of interest can occur when a person or a member of a person's family has an existing or potential interest, or relationship which impairs, or might appear to impair, the person's independent judgement. Family members include a spouse, parents, siblings, children, and others living in the same household.

Workforce members at Director level or above must complete a *Conflict of Interest Statement* and a *Disclosure Statement* upon hire, promotion, when a new conflict arises, and at least annually thereafter. Statements are maintained by the HR department.

Certain relationships with an entity which does business with or directly/indirectly competes with CHNW/CHPW may create a conflict of interest or appearance of conflict of interest. A few examples include:

- Serving as an officer, director, employee, or independent contractor of such an entity.
- Owning or controlling (directly or indirectly) 5% or more of the equity interests of such an entity.
- Receipt of gifts or other favors from such an entity.

A conflict of interest is not inherently illegal or unethical and does not necessarily mean the conflict is damaging for CHNW/CHPW. Each of the following examples may be permissible given the appropriate disclosure and approval:

- A Board member owns a business that provides print services for CHPW member materials.
- A Board member leases real estate to CHPW.
- A Board member applies for employment with CHPW.

These examples can be managed with appropriate disclosure and decision-making. Workforce members should seek clarification from their supervisor, HR, or the Compliance Officer any time they have questions regarding whether a situation presents a potential conflict of interest.

For More Information:

- [Conflict of Interest Policy](#) (EE105)

Compliance Anonymous Reporting

Compliance Program

Compliance Hotline: 1-800-826-6762

chpw.ethicspoint.com

COMMUNITY HEALTH PLAN of Washington™

The power of community

CHPW provides access to a confidential, anonymous **Compliance Hotline** for workforce members to report instances of suspected or detected non-compliance, potential FWA, and other compliance and ethics concerns. The Hotline is operated and available 24 hours a day, seven days a week at **(800) 826-6762**, by NAVEX (vendor). You can also make an anonymous report online by visiting the Compliance Hotline reporting site at: http://chpw.ethicspoint.com/. You can access the online reporting site with the link above, visiting the 'Compliance Hotline' button from the Employee Quick Links on the inside CHPW home page, and from a link on the Compliance Page on inside CHPW.

To ensure confidentiality and comfort in reporting, the Hotline vendor does not trace or record calls. When you make a report online, you are provided with a 'Report Key' and create a password to follow up on your report. Without these, you will not be able to follow up on your submission. NAVEX is unable to recover this information for you. If you choose to remain anonymous, no one will attempt to identify you. If you choose to identify yourself, CHPW will keep your identity confidential, to the fullest extent possible or allowed by law.

When you make a report, the information is provided to the VP, Compliance Officer and the VP, General Counsel for investigation and resolution. You can request an update on the progress or outcome of the investigation by contacting the Compliance Hotline and using the unique identification number and PIN provided during your initial report, or by logging in to the online reporting tool using the 'Report Key' and password mentioned above.

Reminders and Updates

New P&P SharePoint Site, Templates, and Standards

CHPW is retiring its current ***SharePoint 2010*** (i.e., http://chpsp/) site. As a result, the Compliance department has migrated CHPW's Policies and Procedures (P&Ps) to the new ***SharePoint Online*** environment located at https://chpwa.sharepoint.com/sites/PoliciesandProcedures.

The Compliance team is taking advantage of this opportunity to roll out refreshed P&P and Desk Procedure (DP) templates, an updated Style Guide, and approval process.

The link on **insideCHPW** has been updated to direct you to the new site. **Note:** any favorites/bookmarks you've saved in your browser for the old site will need to be updated, including any hyperlinks within your documents.

Visit the new P&P SharePoint site or the Policy and Procedure Approval Process Procedure (CO305) for more information.

New IS&T Cybersecurity Email

IS&T has a new email address that workforce members can use for cybersecurity questions or to contact the IS&T Infosec team: CyberSecurity@chpw.org.

Annual Compliance Program Training and Standards of Conduct Attestation

CHPW assigned annual Compliance Program Training, including the annual Standards of Conduct attestation to all workforce members in April 2021. Training must be completed by **Friday, November 26, 2021**.

To date, approximately 76% of workforce members have completed training.

Training is assigned through UKG Pro. Contact compliance.training@chpw.org if you have any questions or issues with the training modules.

Recently Updated P&Ps:

- Advancce Directives Policy (CO291)
- Compliance Education Program Policy (CO293)
- False Claims and Whistleblower Protections Policy (CO310)
- Privacy Incidents and Breach Notifications Procedure (CO312)
- HIPAA Security Policy (CO330)
- Compliance Audit Policy (CO363)
- Delegated Vendor Oversight (DVO) Program Description